REMARKS

This paper is responsive to the Office Action dated September 27, 2003. All rejections of the Examiner are respectfully traversed. Reconsideration and further examination are respectfully requested.

At paragraph 5 of the Office Action, the Examiner rejected claims 1-8, 15-22, and 26-49 for anticipation under 35 U.S.C. 102 by United States patent number 5,748,736 of Mittra ("Mittra"). Applicants respectfully traverse this rejection.

Mittra discloses a system for secure multicast group communication via multicast or broadcast transmission. As shown in Figs. 1-3, the security group of Mittra appears to cover a hierarchy of multicast networks. Mittra expressly describes a secure multicast group consisting of senders, receivers, a group security controller (GSC), and at least one trusted intermediary (TI) server. See column 4 beginning at line 6. In paragraph 5 of the Office Action, the Examiner asserts that the secure multicast group of Mittra includes multiple domains.

Beginning at line 61 of column 9, Mittra indicates the possible use of three types of keys used in embodiments of the Mittra system. The first possibility is a group key ("Kgrp") that is used to encrypt messages to the secure multicast group. This key is a key known by the secure multicast group of Mittra, which, as above explained, covers a hierarchy of multicast networks. Accordingly, Kgrp is known to multiple multicast networks. A second key proposed for use by Mittra is one that is unique between a sender and the GSC ("Ksender-GSC"). This key agreed upon and known by only a single sender and the GSC. If Ksender-GSC is used for transmission to the GSC, then the GSC operates to decrypt the message, and then re-encrypt the message using the Kgrp before retransmitting the message to the secure multicast group.

Thirdly, Mittra describes the possibility of using a key randomly selected by either the sender or by the GSC, included in the message sent to the GSC, and encrypted using either Kgrp or Ksender-GSC. Processing of messages including such a random key may consist of decrypting and re-encrypting the random key, while the message itself is encrypted only with the random key.

Nowhere in Mittra is there disclosed or suggested any system or method for implementing multicast security in a given multicast domain with one or more network devices, that includes:

> . . .
> receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;
> ***decrypting the received multicast traffic with the global key to produce decrypted multicast traffic***;
> ***encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only to the given multicast domain***; and
> forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. (emphasis added)

As in the present independent claim 1. Analogous features are also found in the present independent claims 15, 26, 34 and 42. If the secure multicast group of Mittra includes multiple multicast networks, Mittra accordingly provides no hint or suggestion of any system or method that decrypts from encryption by such a group, and re-encrypts using a local key known only to one multicast domain, as in the present independent claims. In contradistinction, Mittra teaches the possibility that a key unique to a sender and the GSC is initially used to encrypt the message ("Ksender-GSC"), and then the message is decrypted and re-encrypted using the group key ("Kgrp"). The decryption and re-encryption of a message in Mittra thus provides no hint or

suggestion of even the desirability of decrypting from a global key followed by re-encryption using a local key, *available only to the given multicast domain*, as in the present independent claims.

For the reasons stated above, Applicants respectfully urge that Mittra does not disclose or suggest all the features of the present invention as set forth in independent claims 1, 15, 26, 34 and 42. Accordingly, Applicants respectfully submit that Mittra does not anticipate independent claims 1, 15, 26, 34 and 42 under 35 U.S.C. 102. As to claims 2-8, 16-22, 26-33, 35-41, and 43-49, they each depend from claims 1, 15, 26, 34 and 42, and are believed to be patentable over Mittra for at least the same reasons.

At paragraph 6, the Examiner rejected claims 9-14 and 23-25 as being obvious under 35 U.S.C. 103, citing the combination of United States patent number 6,331,983 of Haggerty et al. ("Haggerty et al.") and "The Microsoft Computer Dictionary", 5th Edition ("Microsoft Computer Dictionary"). Applicants respectfully traverse this rejection.

Haggerty et al. disclose a system for establishing connections in a switch-based communications network for multicast traffic. As described in Haggerty et al., a source receives a multicast packet on an access port from a source host, determines a group address in the multicast packet, and composes and sends a "sender present" message to other switches on its network ports. The receiving switches of the Haggerty et al. system then determine whether a local host wishes to join the group and if so, send a map message back toward the source switch on a predetermined path between the receiving switch and the source switch. The Microsoft Computer Dictionary discloses that encryption prevents unauthorized access, and that one or more keys may be used to perform encryption.

Claims 9 and 23 have been amended to depend from independent claims 1 and 15, respectively. Applicants respectfully urge that, like Mittra, the combination of Haggerty et al. and Microsoft Computer Dictionary fails to disclose or suggest any system or method for implementing multicast security in a given multicast domain with one or more network devices, that includes:

> . . .
>
> receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast domain and one or more other multicast domains;
>
> ***decrypting the received multicast traffic with the global key to produce decrypted multicast traffic***;
>
> ***encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only to the given multicast domain***; and
>
> forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. (emphasis added)

as in the present independent claims 1 and 15, from which claims 9-14 and 23-25 depend.

For these reasons, Applicants respectfully urge that the combination of Haggerty et al. and Microsoft Computer Dictionary does not disclose or suggest all the features of the present independent claims 1 and 15, from which claims 9-14 and 23-25 depend. Accordingly, Haggerty et al. and Microsoft Computer Dictionary do not form a *prima facie* case of obviousness with regard to independent claims 1 and 15. As to claims 9-14 and 23-25, they each depend from claims 1 and 15, and are respectfully believed to be patentable over Haggerty et al. and Microsoft Computer Dictionary for at least the same reasons. Reconsideration of all pending claims is respectfully requested.

For these reasons, and in view of the above amendments, Applicants respectfully request that the Examiner's rejections be withdrawn. This application is now considered to be in condition for allowance and such action is earnestly solicited.

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone David A. Dagg, Applicants' Attorney at 617-630-1131 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

JANUARY 27 2005
Date

David A. Dagg, Reg. No. 37,809
Attorney/Agent for Applicant(s)
Steubing McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-111